UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/940,982	08/29/2001	Takashi Endo	NIT-295	5993

24956 7590 05/08/2006

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 05/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/940,982	ENDO ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 April 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 April 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. A response was received on 03 April 2006. By this response, Claims 1-5 have been amended. Nonelected Claims 9-17 have been canceled. No new claims have been added. Claims 1-8 are currently pending in the present application.

Response to Arguments

2. Applicant's arguments filed 03 April 2006 have been fully considered but they are not persuasive.

Claims 1-8 were rejected on the ground of nonstatutory obviousness-type double patenting as unpatentable over claim 14 of US Patent 6615354 in view of Jaffe et al, US Patent 6510518, and were also rejected under 35 U.S.C. 103(a) as unpatentable over applicant admitted prior art in view of Jaffe et al, US Patent 6510518.

Regarding the double patenting rejection, the Examiner first notes that the Terminal Disclaimer received 03 April 2006 has NOT been accepted because the patent being disclaimed has been incorrectly identified, as noted below. Therefore the disclaimer does not overcome the double patenting rejection.

Further regarding the double patenting rejection, and also in reference to the rejection under 35 U.S.C. 103(a), Applicant additionally argues that Jaffe has been interpreted incorrectly (see page 17 of the present response). Although Applicant concedes that Jaffe teaches that data to be processed can have a constant Hamming

weight to protect against side-channel attacks (pages 18-19 of the present response), Applicant additionally argues that there is no suggestion in the Jaffe reference "to make constant the Hamming weight for the data for disturbance" (page 19 of the present response, emphasis in original). However, the Examiner respectfully disagrees. The Examiner believes that the teaching of Jaffe would reasonably suggest that the constant Hamming weight representation would be used for all data in a system, including both the "data to be processed" and the "data for disturbance" in the admitted prior art. In particular, the Examiner notes that the various constant Hamming weight representations use multiple (at least two) bits to represent a single TRUE or FALSE value (see, for example, Jaffe, column 5, lines 4-22), whereas the traditional representation is a single 1 bit to represent a TRUE value and a single 0 bit to represent a FALSE value (as noted in Jaffe, column 4, lines 62-66). If one represented the "data to be processed" in a constant Hamming weight representation but used a traditional representation for the "data for disturbance", as suggested by Applicant's arguments (pages 19-20 of the present response), then the two representations would be incompatible because there would not be a bit-to-bit correspondence of logic values due to the longer representations in the constant Hamming weight scheme. Therefore, the Examiner believes that the teachings of Jaffe would reasonably suggest using a constant Hamming weight representation for either ALL or NONE of the data in a system such as the one admitted as prior art, instead of for some pieces of data but not others.

Therefore, for the reasons detailed above, the Examiner maintains the rejections as set forth below.

Drawings

3. The objections to the drawings are withdrawn in light of the new drawings filed and the amendments to the specification.

Specification

4. Although Applicant has corrected some of the errors in the disclosure as noted in the previous Office action, the discrepancies noted between the description of Figure 8 and the figure itself have not been addressed.

5. The disclosure is objected to because of the following informalities:

The specification appears to contain minor errors. Specifically, on pages 31-35, there appear to be discrepancies between the description of Figure 8 and the figure itself. For example, on page 31, lines 24-26, of the specification as filed, the description of step 808 in the specification states that the subscript of the array (b) is incremented; however, step 808 in Figure 8 shows b set equal to 0.

Appropriate correction is required. Applicant is reminded that the above is not to be considered an exhaustive list of errors. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors.

Applicant's cooperation is again requested in correcting any errors of which applicant may become aware in the specification.

Terminal Disclaimer

6. The terminal disclaimer filed on 03 April 2006 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of US Patent 6,615,354 has been reviewed and is NOT accepted.

7. The terminal disclaimer does not comply with 37 CFR 1.321(b) and/or (c) because:

> The application/patent being disclaimed has been improperly identified since the number used to identify the patent being disclaimed is incorrect. The correct number is 6,615,354 (and not 6,510,518 as listed).

Double Patenting

8. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

9. Claims 1-8 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 14 of U.S. Patent No. 6615354 in view of Jaffe et al, US Patent 6510518.

Claim 14 of the conflicting patent is directed to a method that corresponds substantially to the apparatus claimed in Claims 1 and 2 of the present application. However, the conflicting patent does not explicitly disclose the limitation of Claim 1 that the disturbance data and processed disturbance data each have a constant Hamming weight. Jaffe discloses that data used in cryptographic processing can be represented using a constant Hamming weight representation (column 4, line 55-column 5, line 30). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of the conflicting patent to include constant Hamming weight data, in order minimize the information leaked from cryptosystems by power consumption fluctuations (see Jaffe, column 2, lines 44-48). Claims 4 and 5 contain limitations similar to those of Claim 2, and thus correspond to limitations in Claim 14.

In reference to Claim 3, Jaffe further discloses that each bit has a logic value of 1 or 0 at a probability of 50% (see the table at column 9, noting the representations s_8; see also column 8, lines 41-45). In reference to Claim 6, Jaffe further discloses means

for generating random numbers each having a Hamming weight equal to half the numbers of bits include in the random number, means for inverting bits of data, and means for concatenating a random number with data output by the means for inverting (see the table at column 9, noting the representations s_8; see also column 8, lines 41-45). In reference to Claim 7, Jaffe further discloses a Hamming weight computation means, a Hamming weight examination means, and a constant Hamming weight assurance means (see column 4, line 55-column 5, line 30, where the representations guarantee a constant Hamming weight). In reference to Claim 8, Jaffe further discloses means used to generate partial random numbers with uniform bit counts and means for concatenating the partial random numbers to result in a final random number (see the table at column 9; Figure 1; and column 7, line 57-column 8, line 65). Therefore it would have been obvious to further include the limitations of Jaffe for the reasons set forth above in reference to Claims 1 and 2.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over applicant admitted prior art in view of Jaffe et al, US Patent 6510518.

In reference to Claim 1, Applicant admits as prior art an apparatus including a data transform means transforming input data by using disturbance data to generate transformed data, a transformed data processing means for carrying out predetermined processing on the transformed data to generate processed transformed data, and a data inverse transform means for carrying out inverse transformation processing on the processed transformed data using processed disturbance data to generate processed data (see page 21, lines 1-12 of the present application). However, Applicant admits that such prior art does not explicitly disclose that the disturbance data and the processed disturbance data have a constant Hamming weight.

Jaffe discloses that data used in cryptographic processing can be represented using a constant Hamming weight representation (column 4, line 55-column 5, line 30). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of the prior art to include constant Hamming weight data, in order minimize the information leaked from cryptosystems by power consumption fluctuations (see Jaffe, column 2, lines 44-48).

In reference to Claim 2, Applicant admits that the prior art further discloses that the processed disturbance data can be generated by carrying out the predetermined processing on the disturbance data (page 21, lines 6-8 of the present application).

In reference to Claim 3, Jaffe further discloses that each bit has a logic value of 1 or 0 at a probability of 50% (see the table at column 9, noting the representations s_8; see also column 8, lines 41-45).

In reference to Claim 4, Applicant admits that the prior art further discloses generating processed disturbance data by carrying out the predetermined processing o the disturbance data (page 21, lines 6-8 of the present application). Further, it is well known that data can be pre-computed.

In reference to Claim 5, Applicant further admits that the processed disturbance data can be generated by carrying out the predetermined processing on the disturbance data (page 21, lines 6-8 of the present application).

In reference to Claim 6, Jaffe further discloses means for generating random numbers each having a Hamming weight equal to half the numbers of bits include in the random number, means for inverting bits of data, and means for concatenating a random number with data output by the means for inverting (see the table at column 9, noting the representations s_8; see also column 8, lines 41-45).

In reference to Claim 7, Jaffe further discloses a Hamming weight computation means, a Hamming weight examination means, and a constant Hamming weight assurance means (see column 4, line 55-column 5, line 30, where the representations guarantee a constant Hamming weight).

In reference to Claim 8, Jaffe further discloses means used to generate partial random numbers with uniform bit counts and means for concatenating the partial random numbers to result in a final random number (see the table at column 9; Figure 1; and column 7, line 57-column 8, line 65).

Conclusion

12. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER